REMARKS

The Claim amendments

The claims are amended to recite wireless network instead of cellular network. Moreover, claims 3, 5 and 12 are amended in view of the points raised on page 3 of the office action.

The Problem in the Art

In general, DRM protection is based on the principle that every end-entity able to consume DRM protected content is equipped with a cryptographic key, which usually is unique for every end-entity.

DRM protected content is distributed, possibly together with a set of consumption rights, in encrypted form. Thus, only authorized parties, usually those that have paid for the content, are able to consume the content. This is done, for example, by encrypting the content with the public key matching the recipient's private DRM key (asymmetric key encryption). For practical reasons, usually a hybrid scheme is chosen, wherein DRM protected content is encrypted under a content encryption key (CEK) using symmetric encryption. The CEK in turn is then encrypted with the public DRM key matching the recipient's private DRM key. The CEK may be accompanied by consumption rights (which may also be encrypted) expressing the usage rules for the DRM protected content.

The effect is the same for both approaches, i.e., only authorized parties are able to consume the DRM protected content (if implemented securely and correctly). The two approaches, however, also share a drawback originating from the fact that every end-entity is equipped with a unique DRM key: content (or the CEK) has to be personalized for every device prior to consumption.

Usually, DRM content is protected, i.e., encrypted, (and therefore personalized) by the network side for various reasons, e.g., to guarantee payment for the content. Typically, the network infrastructure has a server for personalizing content transported in the wireless network. The network centric nature of current approaches, however, is not very suitable for certain types of content, e.g., free content. The most prominent example being content intended for preview purposes.

Because of this, peer-to-peer forwarding of DRM protected content and immediate consumption thereafter is not possible. Either the recipient of DRM protected content that has been forwarded in a peer-to-peer fashion must establish connection to the network infrastructure before being able to consume the content, or the sender must in the first place send the content to the network infrastructure which will personalize the content for and route it to the recipient. (The latter case, however, is not classified as true peer-to-peer superdistribution anymore.)

In addition, DRM implementations in the Internet world generally do not offer the possibility to superdistribute content in a peer-to-peer fashion without network access, e.g., for preview purposes prior to purchasing.

In view of the aforementioned, there is a need in the art to solve the problem of user-friendly peer-to-peer forwarding of DRM protected content (or CEK) without requiring network access for personalization of the DRM protected content (or CEK) while at the same time enabling the detection and prevention of distributing pirated DRM content.

This is the problem the inventor faced.

The Claimed Solution

The inventor recognized the aforementioned problem in the art problem and provided a solution to the same.

In its broadest sense, the solution is in the form of a new technique featuring forwarding peer-to-peer content between two mobile phones communicating in a wireless network via a network infrastructure, where a mobile phone sender sends an initial message having an international mobile equipment identity, a mobile phone sender name or mobile station international integrated subscriber digital network number and encrypts protected content or content encryption key, and a mobile phone recipient consumes the protected content without requiring content personalization assistance from the network infrastructure of the wireless network.

In operation, as recited, e.g. in claims 3-7, the mobile phone recipient can send a device certificate having a public key to a wireless sender, the mobile phone sender can personalize the protected content or content encryption key for the mobile phone recipient, and the personalizing may include: encrypting the content or content encryption key using the public key of the mobile phone recipient; signing encrypted content or content encryption key using a private key of the mobile phone sender; and sending the protected content or content encryption key together with a device certificate of a wireless sender to the mobile phone recipient. The mobile phone recipient can also verifies forwarded protected content received from the mobile phone sender by: verifying the device certificate of the mobile phone sender; and applying a private key of the mobile phone recipient in order for the recipient to consume the protected content.

The Contribution to the State of the Art

The claimed invention provides an important contribution to the wireless world and solves a problem particularly important to the mobile network domain, by defining a process that enables peer-to-peer distribution of DRM protected content that must be personalized for the recipient prior to consumption. With the claimed invention, the sending terminal is able to personalize the content in a non-network centric fashion.

The claimed invention also greatly obstructs the circulation of pirated DRM content by requiring both the wireless sender terminal and the wireless receiver terminal to be tampered with in order to exchange pirated DRM content without the possibility of being detected. Thus the claimed invention reduces the number of rogue terminals participating in the distribution of pirated DRM content.

By applying a combination of accountability and non-repudiation together with rewarding honest terminals, the claimed invention reverses the reversed threat model of DRM, and provides a way to gather information for forensic analysis, thus enabling identification of terminals and prosecution of distributors of pirated DRM content. In effect, the claimed invention permits rewarding honest end-entities reporting distributors of pirated DRM content to the DRM system operator. Thus, the claimed invention actively reduces the number of end-entities consuming and exchanging pirated DRM content, crucial to keeping the fraud level below some threshold vital to businesses to remain profitable.

Also, the overall mechanism for identifying end-entities distributing pirated DRM content and rewarding honest end-entities reporting distributors of pirated DRM content is new and unique. By reversing the reversed threat model, now not every user is a potential adversary anymore, rather every user is a potential DRM enforcement agent.

In the case where multiple devices share the same private DRM key (so called group or domain concept), content must be personalized for every set, that is a group or domain, of devices sharing the same private DRM key prior to consumption. In this case, the invention enables the user-friendly peer-to-peer distribution of DRM protected content between devices belonging to different sets.

The Traversal

The main independent claims are rejected based on a new three reference combination, including Safadi, et al., Bloebaum and Vogel.

However, it is respectfully submitted that Safadi, et al., Bloebaum and Vogel. do not either recognize the problem being addressed by the claimed invention, or teach or suggest a solution to said problem.

Safadi has been discussed and distinguished recently in the March 11th response accompanying the RCE. Safadi, et al. addresses the problem related to allowing a consumer to transfer content among multiple devices in a transparent manner, transparent to the content type and the devices involved, while limiting the distribution and further playback of copyright-protected content, as described in Safadi, et al., paragraph [0008] . To solve this problem Safadi, et al. discloses apparatus having a playback area network (PAN) 20 for coupling a personal versatile recorder (PVR) 10 to auxiliary device or components 30. Safadi, et al. describes the PVR 10 as a digital compression device that functions as a caching and distribution gateway for the transfer of multimedia content from the system operator and affiliated content provider, as set forth on page 2, paragraph [0030]. The PVR 10 may be either integrated into a set-top terminal or housed separately as a stand-alone unit, as set forth on page 2, paragraph [0031]. Safadi et al. describes that its receiver/playback device 30 may take the form of a mobile phone. The PAN 20 may be a wired or wireless network that is suitable for transporting encrypted multimedia content from the PVR 10 to the receiver playback device 30 via a standard protocol, e.g. a Secure Socket Layer (SSL) protocol.

It is respectfully submitted that Safadi, et al. does not recognize or provide a solution to the problem of user-friendly peer-to-peer forwarding of DRM protected content (or CEK) without requiring network access for personalization of the DRM protected content (or CEK) while at the same time enabling the detection and prevention of distributing pirated DRM content.

On page 5 of the outstanding office, the reasoning recognizes that that Safadi is clearly missing some key pieces to the claimed invention, including the peer-to-peer forwarding of encrypted content from the mobile phone sender along with the message having an IMEI, a mobile sender name or mobile station international integrated subscriber digital network number, as well as the peer-to-peer consumption of such encrypted content by the mobile phone recipient without requiring assistance from network infrastructure in the cellular network. However, in order to make up for these deficiencies in the teaching of Safadi, the reasoning on page 5 of the outstanding office is citing Bloebaum or Vogel.

However, Bloebaum recognizes that there is problem related a GPS-equipped cellular phone that is situated in a cell not having access to GPS-related information, and the need to be able to provide this information from another source, as described in Bloebaum, the paragraph bridging columns 1-2 thereof. To solve this problem, Bloebaum discloses a peer-to-peer information exchange for mobile communications devices, where friends can share files for applications such as games or music between cell phones. Clearly, the files for applications are not encrypted before being forwarded, and encrypted content is not consumed by a mobile phone recipient without requiring assistance from network infrastructure in the wireless network, both as claimed. Further, it is respectfully submitted that, similar to Safadi, et al., Bloebaum also does not recognize or provide a solution to the problem of user-friendly peer-to-peer forwarding of DRM protected content (or CEK) without requiring network access for personalization of the DRM protected content (or CEK) while at the same time enabling the detection and prevention of distributing pirated DRM content.

Moreover, Vogel discloses a GSM based system in which the international mobile station equipment number uniquely identifies mobile stations internationally.

Similar to Bloebaum, files for applications are not encrypted before being forwarded, and encrypted content is not consumed by a mobile phone recipient without requiring assistance from network infrastructure in the wireless network , both as claimed. Further, it is respectfully submitted that, similar to Safadi, et al. and Bloebaum, Vogel also does not recognize or provide a solution to the problem of user-friendly peer-to-peer forwarding of DRM protected content (or CEK) without requiring network access for personalization of the DRM protected content (or CEK) while at the same time enabling the detection and prevention of distributing pirated DRM content.

In view of this, it is respectfully submitted that all three cited prior art references do not teach or suggest the whole thrust of the claimed invention, including peer-to-peer forwarding of encrypted content from a mobile phone sender along with a message having an IMEI, a mobile sender name or mobile station international integrated subscriber digital network number, along with peer-to-peer consumption of such encrypted content by a mobile phone recipient without requiring assistance from network infrastructure in a wireless network, as claimed.

Regarding the other issues raised by the Examiner, we will change "cellular" back to --wireless-- network.

The remaining claims depend directly or indirectly from the main independent claims, contain all the limitations thereof, and are deemed patentable over the cited prior art for all the same reasons.

For all these reasons, the claimed invention is patentable over the cited prior art.

Reconsideration and early allowance is earnest solicited.

Respectfully submitted,

/William J. BARBER/
William J. Barber
Attorney for the Applicant
Registration No. 32,720

WARE, FRESSOLA, VAN DER SLUYS
& ADOLPHSON LLP
Customer No. 004955
Bradford Green, Building Five
755 Main Street, P.O. Box 224
Monroe, CT 06468
(203) 261-1234